



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,593	04/06/2001	Jari Pekka Hamalainen	460-006859-US (C01)	3070
2512	7590	12/04/2009		
Perman & Green, LLP 99 Hawley Lane Stratford, CT 06614				
EXAMINER				
SHAW, YIN CHEN				
ART UNIT		PAPER NUMBER		
2439				
MAIL DATE		DELIVERY MODE		
12/04/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/827,593

Applicant(s)

HAMALAINEN ET AL.

Examiner

Yin-Chen Shaw

Art Unit

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 August 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) See Continuation Sheet is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 9, 21, 23-26, 28, 31-48, 55-59, 61-64, 66-70, 74-82, 84-94, 96, 122, 124-126, 128-130, and 132-156 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 02/05/2009.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Continuation of Disposition of Claims: Claims pending in the application are 19,21,23-26,28,31-48,55-59,61-64,66-70,74-82,84-94,96,122,124-126,128-130 and 132-156.

DETAILED ACTION

1. This written action is responding to the amendment dated on 08/05/2009.
2. Claims 19, 21, 35-43, 58-59, 61, 66-70, 74-82, 84-94, 96, 122, 124-126, 128, 130, 132, 136-137, and 147-156 has been amended. Claims 27, 49-53, 65, 97, 123, 127, and 131 are further canceled from examination. The status of all other claims remains previously presented.
3. Claims 19, 21, 23-26, 28, 31-48, 55-59, 61-64, 66-70, 74-82, 84-94, 96, 122, 124-126, 128-130, and 132-156 have been examined and rejected.
4. Claims 19, 21, 23-26, 28, 31-48, 55-59, 61-64, 66-70, 74-82, 84-94, 96, 122, 124-126, 128-130, and 132-156 are pending.

Response to Arguments

5. Applicant's amendment, filed on Aug. 05, 2009, has claims 19, 21, 35-43, 58-59, 61, 66-70, 74-82, 84-94, 96, 122, 124-126, 128, 130, 132, 136-137, and 147-156 amended, claims 27, 49-53, 65, 97, 123, 127, and 131 canceled, and the status of all other claims remains previously presented. Among the amended claims, claims 19, 59, 82, 85, 94, 122, 132, 136, and 156.
6. Examiner respectfully disagrees with Applicant's argument regarding the skilled person would not be motivated to combine the teachings of Sasuta and Talbot. Although Sasuta's teaching is related to have encryption control/indication information transmitted through control channel to

indicate whether of communication in secure or non-secure mode should take place, it also uses the working channel to transmit data with an option of marking the communication secure/encrypted (see Col. 4, lines 17-29 and Col. 5, 47-50 from Sasuta). Talbot, meanwhile, teaches the option of have secured or unsecured transmission between units (see Col. 11, lines 13-24; Col. 11, line 59 to Col. 12, line 3). Thus, the combination of Sasuta and Talbot, contrary to Applicant's argument, would result the working channel transmitting encrypted or unencrypted information, and this meets with the claimed invention.

7. Applicant's argument regarding cipher mode indicator in the mobile station is moot in view of the new ground of rejections based on the newly found reference by Rasmussen et al. (U.S. Patent 5,222,136), which discloses disclosing a display of a communication device is utilized for indicating the mode of (encrypted or decrypted) communication it is currently operating in (see Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.). Please refer rejections below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 156 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. (U. S. Patent 5,502,767) and further in view of Talbot (U.S. Patent 4,555,805).

As per claims 156:

Sasuta et al. disclose "an apparatus for use in a mobile station, the apparatus comprising:

a cipher indication memory block comprising a cipher mode indication data field, the cipher mode indication data field for holding cipher indication data indicative of a ciphering mode used in communication between a mobile station and a mobile communication network" in (Col. 3, lines 23-39; Col. 3, line 60 to Col. 4, line 38; and Col. 5, lines 3-18 from Sasuta et al.).

an output for providing the cipher indication data to a user interface block of the mobile station responsive to a cipher mode enquiry from the user interface block (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50, *where users are indicated that the cipher mode is to be applied based on toning signal and are inquired whether the cipher mode is to be applied at higher cost rate*).

Therefore, it would have been obvious at the time of invention was made for one having ordinary skill in the art to modify

Sasuta's teaching with Talbot since one would be motivated to maintaining secure information synchronization on a control channel that will not reduce the efficiency of a secure radio communication system (Col. 2, lines 32-34 from Sasuta et al.).

9. Claims 19, 21, 23, 28, 31, 36, 44, 46-48, 55-59, 61-62, 66, 68, 74, 77-79, 81-82, 84-87, 90-91, 93-94, 96, 122, 124, 128, 132-134, 136-139, 142-143, and 148, and 152-153 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. (U. S. Patent 5,502,767) and further in view of Talbot (U.S. Patent 4,555,805) and Rasmussen et al. (U.S. Patent 5,222,136).

As per claims 19, 59, and 82:

Sasuta et al. disclose "a method and apparatus for use within a mobile station for determining a ciphering mode to be used in communication between a mobile communication network and a mobile station, the mobile station being capable of communication in at least one enciphered mode of communication and in at least one enciphered mode of communication" in (Col. 3, lines 23-39; Fig. 1), "the method comprising:

"monitoring at the mobile station control signals received from the mobile communication network to detect a cipher mode command

message, the cipher mode command message requesting the mobile station start encipher" (Col. 3, lines 23-39; Col. 3, line 60 to Col. 4, line 17; Fig. 1);

"responsive to reception of cipher mode command message in the monitored control signals from the mobile communication work, start enciphering in the mobile station" (Col. 4, lines 18-30 and 60-65 and Col. 5, lines 41-43).

Sasuta et al. do not expressly disclose the remaining limitation of the claim.

However, Talbot discloses "indicating that the mobile communication network is in ciphering mode of communication" (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50, *where users are being indicated that the cipher mode is to be applied with completion toning signal and higher cost*). Therefore, it would have been obvious at the time of invention was made for having ordinary skill in the art to modify Sasuta's teaching with Talbot since one would be motivated to maintaining secure information synchronization on a control channel that will not reduce the efficiency of a secure radio communication system (Col. 2, lines 32-34 from Sasuta et al.).

Sasuta et al. and Talbot do not expressly disclose the limitation regarding the cipher mode indicator for providing the indication to user is in the mobile station.

However, Rasmussen et al. disclose that the limitation regarding the cipher mode indicator for providing the indication to user is provided in the mobile station by teaching the display of an RF communication telephonic device is utilized for indicating the mode of (encrypted or decrypted) communication it is currently operating in (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

Therefore, it would have been obvious at the time of invention was made for one having ordinary skill in the art to modify the teaching from Sasuta and Talbot with Talbot since one would be motivated to protect each type communications device without expensively using separate security systems (Col. 1, lines 66-68 from Rasmussen et al.).

As per claims 21 and 61:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 19 and 59, further comprising the step of indicating that to a user of the mobile station that the mobile communication network is operating in an unciphered mode of communication, using the cipher mode indicator provided

in the mobile station (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.) if no cipher mode command message is detected at the mobile station in the monitored control signals received from the mobile communication network" in and (Col. 4, lines 9-11 from Sasuta et al.) and (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50 from Talbot).

As per claims 23 and 62:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 19 and 59, wherein the apparatus is configured to determine the ciphering mode to be used in communication between the mobile communication network and the mobile station during establishment of communication between the mobile communication network and the mobile station (Col. 4, lines 39-59 from Sasuta et al.) and (Col. 10, lines 9-30 from Talbot).

As per claims 28 and 68:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 19 and 59, further comprising indicating a ciphering mode, a change in ciphering mode to a user of the mobile station" in (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50 from Talbot).

As per claims 36 and 74:

Sasuta et al., Talbot, and Rasmussen et al. disclose "an apparatus according to claims 19 and 59, wherein the mobile stations comprises of: a radio resource management block and a cipher indicator memory block, wherein said means for monitoring signals sent from the mobile communication network to the mobile station and said means for determining if said monitored signals comprise a cipher mode command message are arranged in the radio resource management block and a cipher mode indication data field is maintained in the cipher indication memory block, the radio resource management block being further arranged to set a value of the cipher mode indication data field to correspond with cipher indication data in said cipher mode command message received from the mobile communication network" (Col. 3 line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.) and (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50 from Talbot).

As per claims 44 and 46-47:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 19, wherein the mobile station is capable of a

first type of communication and an indication of a cipher mode". And indicating a ciphering mode of each of said first and second types and change of modes of communications to a user of the mobile station (Col. 7, lines 7-25 and Fig. 3 from Rasmussen et al.).

As per claim 48:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 19, wherein a first mobile station and a second mobile station are in communication with each other through at least one mobile communication network, the method comprising indicating the ciphering mode between the mobile communication network and the first mobile station to a user of the second mobile station" (Col. 3 line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.) and (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50 from Talbot).

As per claim 55:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 19, comprising using the mobile station in communication with a terminal in a fixed line communication network, and the method further comprising indicating a ciphering

mode used in communication between the fixed line communication network and the terminal in the fixed line communication network to a user of the mobile station" in (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 32-50; Col. 10, lines 10-22 from Talbot) and (Col. 3, lines 35-39 and Fig. 1 from Sasuta et al.).

As per claim 56:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 55, wherein the mobile station sends an inquiry message to the terminal in the fixed line communication network to determine the ciphering mode used in communication between the fixed line communication network and said terminal in the fixed line network" in (Col. 4, lines 18-29 from Sasuta et al.) and (Col. 3, line 60 to Col. 4, line 12; Col. 10, lines 10-22 from Talbot).

As per claim 57:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 56, wherein if the mobile station does not receive a response to said inquiry message, the mobile station indicates that the ciphering mode is unknown" in (Col. 9 lines 45-50 and 67-68; Col. 10, lines 1-8 from Talbot) and (Col. 5 lines 5-18 from Sasuta et al.).

As per claim 58:

Sasuta et al., Talbot, and Rasmussen et al. disclose “a method according to claim 55, wherein if the mobile station receives a response to said inquiry message, but cannot interpret said response, the mobile station indicates that the ciphering mode is unknown” in (Col. 4, lines 58-68 from Talbot) and (Col. 5, lines 19-29 from Sasuta et al.).

As per claims 77, 79, 81, 87, and 93:

Sasuta et al., Talbot, and Rasmussen et al. disclose “an apparatus according to claims 76, 78, 80, 86, and 92, wherein user interface block is configured to set the cipher mode indicator to a mode corresponding to the ciphering data provided by the cipher indicator memory block” in ((Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 17; Fig. 1 from Sasuta et al.), (Col. 4, lines 40-54; Col. 11, line 59 to Col. 12, line 3; Col. 8, lines 3-25; Col. 9, lines 32-50 from Talbot), and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.)).

As per claims 78, 90, and 91:

Sasuta et al., Talbot, and Rasmussen et al. disclose "an apparatus according to claims 74, 86, and 90, wherein the cipher indicator memory block is configured to send cipher information to the user interface block whenever the value in the cipher indicator memory block is changed" in ((Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 17; Fig. 1 from Sasuta et al.), (Col. 4, lines 40-54; Col. 11, line 59 to Col. 12, line 3; Col. 8, lines 3-25; Col. 9, lines 32-50 from Talbot), and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.)).

As per claim 84:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 82 wherein the cipher mode indicator is further configured to indicate that the mobile communication network is operating in an unciphered mode of communication if no cipher mode command message is detected in the control signals received from the mobile communication network" in (Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 38; Col. 5, lines 13-18; Fig. 1 from Sasuta et al.) and (Col. 4, lines 40-54; Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 32-50; Col. 10, lines 10-22 from Talbot).

As per claims 85 and 94:

Sasuta et al. disclose "a system for determining a ciphering mode to be used in communication between a mobile communication network and a mobile station in the mobile communication network, the mobile station capable of communication in at least one enciphered mode of communication and at least one unciphered mode of communication" in (Col. 3 line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.), the system comprising:

means in the mobile communication network for determining whether an enciphered mode of communication is to be used in communication between the mobile communication network and the mobile station according to a setting of the mobile communication network (Col. 3 line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.);

means in the mobile communication network for sending a cipher mode command message from the mobile communication network to the mobile station in a situation where an enciphered mode of communication is to be used in communication between the mobile communication network and the mobile station, said cipher mode command message requesting the mobile station to

start enciphering (Col. 3, lines 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.);

means in the mobile station for monitoring control signals sent from the mobile communication network to the mobile station to detect a cipher mode command message (Col. 3, lines 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.);

means in the mobile station for starting enciphering in the mobile station responsive to detection of a cipher mode command message in the monitored control signals from the mobile communication network (Col. 4, lines 18-30 and 60-65 and Col. 5, lines 41-43); and

Sasuta et al. do not expressly disclose the remaining limitation of the claim.

However, Talbot discloses "means for indicating a ciphering mode to a user of the mobile station, comprising means for indicating that the mobile communication network is operating in an enciphered mode of communication responsive to detection of a cipher mode command message and means for indicating that the mobile communication network is operating in an unciphered mode of communication if no cipher mode command message is detected in the monitored control signals said monitored signals do not comprise a cipher mode control signal" (Col. 11, line 59 to

Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50 from Talbot).

Therefore, it would have been obvious at the time of invention was made for having ordinary skill in the art to modify Sasuta's teaching with Talbot since one would be motivated to maintaining secure information synchronization on a control channel that will not reduce the efficiency of a secure radio communication system (Col. 2, lines 32-34 from Sasuta et al.).

Sasuta et al. and Talbot do not expressly disclose the limitation regarding the cipher mode indicator for providing the indication to user is in the mobile station.

However, Rasmussen et al. disclose that the limitation regarding the cipher mode indicator for providing the indication to user is provided in the mobile station by teaching the display of an RF communication telephonic device is utilized for indicating the mode of (encrypted or decrypted) communication it is currently operating in (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

Therefore, it would have been obvious at the time of invention was made for one having ordinary skill in the art to modify the teaching from Sasuta and Talbot with Talbot since one would be motivated to protect each type communications device without

expensively using separate security systems (Col. 1, lines 66-68 from Rasmussen et al.).

As per claim 86:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 85, comprising a radio resource management block and a cipher indicator memory block and a user interface block, the cipher mode indicator block comprising a cipher mode indication data field, the radio resource management block being configured to set a value of the cipher mode indication data field to correspond with cipher indication data in a cipher mode command message received from the mobile communication network" in (Col. 3, line 60 to Col. 4, line 17 and Col. 5, lines 5-18 from Sasuta et al.) and (Col. 8, lines 3-25 and Fig. 1 from Talbot)

As per claim 96:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a system according to claim 94, wherein the cipher mode indicator is further configured to indicate that the mobile communication network is operating in an unciphered mode of communication, using the cipher mode indicator provided in the mobile station (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.) if no

cipher mode command message is detected at the mobile station in the monitored control signals received from the mobile communication network (Col. 3, line 60 to Col. 4, line 17; Col. 5, lines 5-18; Fig. 1 from Sasuta et al.) and (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25 from Talbot).

As per claims 122, 132, and 136

Sasuta et al. disclose an apparatus for determining a ciphering mode of communication between a mobile communication network and a mobile station, the mobile station being capable of communication in at least one enciphered mode of communication and at least one unciphered mode of communication (Col. 3, line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.).

Sasuta et al. further disclose the mobile communication network is configured to use an enciphered mode of communication, a cipher mode indicator for indicating that the mobile communication network is configured to use an enciphered mode of communication, and signals sent from the mobile communication network to the mobile station determining if monitored signals comprise a cipher mode control signal (Col. 3,

line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.);

a cipher indication memory block having a cipher mode indication data field, the cipher mode indication data field having a value representative of said cipher mode used in communication between the mobile communication network and the mobile station" in (Col. 3, line 60 to Col. 4, line 17 and Col. 5, lines 5-18 from Sasuta et al.); and

monitoring at the mobile station control signals received from the mobile communication network (Col. 3, lines 23-39; Col. 3, line 60 to Col. 4, line 17; Fig. 1).

Sasuta et al. do not expressly disclose a radio resource management block and other limitations.

However, Talbot discloses a radio resource management block for monitoring signals (Col. 8, lines 3-25; Col. 9, lines 32-50; Fig. 1 from Talbot) and indicating a ciphering mode that the mobile communication network is configured to use an enciphered mode of communication responsive to detection of a cipher mode command message" (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50; Col. 10, lines 10-29 from Talbot).

Therefore, it would have been obvious at the time of invention was made for one having ordinary skill in the art to modify Sasuta's teaching with Talbot since one would be motivated to

maintaining secure information synchronization on a control channel that will not reduce the efficiency of a secure radio communication system (Col. 2, lines 32-34 from Sasuta et al.).

Sasuta et al. and Talbot do not expressly disclose the limitations regarding the cipher mode indicator for providing the indication to user is provided in the mobile station and a user interface block configured to control a cipher mode indicator to inform a user that the mobile communication network is operating in an enciphered mode of communications

However, Rasmussen et al. disclose that the limitations regarding the limitations regarding the cipher mode indicator for providing the indication to user is provided in the mobile station and a user interface block configured to control a cipher mode indicator to inform a user that the mobile communication network is operating in an enciphered mode of communications by teaching the display of an RF communication telephonic device is utilized for indicating the mode of (encrypted or decrypted) communication it is currently operating in (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

Therefore, it would have been obvious at the time of invention was made for having ordinary skill in the art to modify the teaching from Sasuta and Talbot with Talbot since one would be motivated to protect each type communications device without

expensively using separate security systems (Col. 1, lines 66-68 from Rasmussen et al.).

As per claims 31, 66, and 143:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 19, 59, and 136, wherein said means for indicating a ciphering mode used in the communication between the mobile communication network and the mobile station to a user of the mobile station using the display unit ((Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50 from Talbot) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.)).

As per claims 124:

Sasuta et al., Talbot, and Rasmussen et al. disclose "an apparatus according to claim 122, comprising a radio resource management block, the radio resource management block being configured to set a value of the cipher mode indication data field to correspond with cipher indication data in a cipher mode command message received from the mobile communication network" in (Col. 3, line 60 to Col. 4, line 17 and Col. 5, lines 5-18 from Sasuta et al.) and (Col. 8, lines 3-25 and Fig. 1 from Talbot).

As per claims 128:

Sasuta et al., Talbot, and Rasmussen et al. disclose "an apparatus according to claim 124, wherein the cipher indicator memory block is

Configured send cipher information to the user interface block whenever the value in the cipher mode indicator memory is changed" (Col. 3, line 24-39; Col. 3, line 60 to Col. 4, line 17; Fig. 1 from Sasuta et al.) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

As per claims 133:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a system according to claim 94, wherein the ciphering mode to be used in communication between the mobile communication network and the mobile station is specified by an operator of the mobile communication network" in (Col. 10, lines 9-30 from Talbot).

As per claims 134:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a system according to claim 94, wherein communication between the

mobile communication network and the mobile station takes place at least in part over a radio link" in (Fig.1 from Sasuta et al.).

As per claims 137:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 136, wherein the user interface block is configured to control the cipher mode indicator to inform a user that the mobile communication network is configured to use an unciphered mode of communication, if the radio resource management block does not detect a cipher mode command message in the monitored control signals received from the mobile communication network" in (Col. 3, line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.) and (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50; Col. 10, lines 10-29 from Talbot).

As per claims 138:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 136, wherein the mobile station is configured to determine a ciphering mode to be used in communication between the mobile communication network and the mobile station during establishment of communication

between the mobile communication network and the mobile station" in (Col. 3, line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.).

As per claims 139:

Sasuta et al., Talbot, and Rasmussen et al. disclose a mobile station according to claim 136, wherein the mobile station is configured to determine a ciphering mode to be used in communication between the mobile communication network and the mobile station prior to establishment of communication between the mobile communication network and the mobile station" in (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50; Col. 10, lines 10-29 from Talbot).

As per claims 142:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 136, wherein the mobile station is configured to inform a user of a change in ciphering mode" in (Col. 3, line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.) and (Col. 11, line 59 to Col. 12, line 3 and Col. 8, lines 3-25; Col. 9, lines 39-50; Col. 10, lines 10-29 from Talbot).

As per claims 148:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 136, wherein the mobile station comprises a cipher indication memory block and the radio resource management block is configured to set a cipher mode indication data field of the cipher indication memory block to correspond with cipher indication data in a cipher mode control signal received from the mobile communication network" in (Col. 8, lines 3-25; Col. 9., lines 39-50 and 67-68; Col. 10, lines 1-8; and Fig. 1 from Talbot) and (Col. 3, line 24-39; Col. 3, line 60 to Col. 4, line 38; Fig. 1 from Sasuta et al.).

As per claims 152:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a mobile station according to claim 148, wherein the cipher indicator memory block is configured to send cipher information to the user interface block whenever the said value in the cipher mode indicator memory block is changed" in ((Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 38; Fig. 1 from Sasuta et al.) and (Col. 4, lines 40-54; Col. 11, line 59 to Col. 12, line 3; Col. 8, lines 3-25; Col. 9, lines 32-50 from Talbot) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.)).

As per claims 153:

Sasuta et al., Talbot, and Rasmussen et al. disclose a mobile station according to claim 152, wherein the user interface block is configured to set the cipher mode indicator to a mode corresponding to the cipher information provided by the cipher mode indicator memory block (Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 38; Fig. 1 from Sasuta et al.) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

10. Claims 24-26, 63-64, and 135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, and Rasmussen et al. and further in view of Billstrom et al, US Patent No 5590133, hereinafter "Billstrom".

As per claims 24-25 and 63-64:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 19, 24, 59, and 63". Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose "comprising determination of the ciphering mode to be used in communication prior to establishment of data communication between the mobile communication network and the mobile station is performed by means of a location update procedure".

Nevertheless, Billstrom discloses the "apparatuses and Mobile stations for providing packet data communication in digital TDMA Cellular Systems" invention, which teaches "the determination of the ciphering mode to be used in data communication prior to establishment of data communication between the mobile communication network and the mobile station is performed by means of a location update procedure" in (Col 9 lines 20-50, and Col 10 lines 45-61).

Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art at the time of invention to incorporate Billstrom with ciphering mode teaching in Sasuta et al., Talbot, and Rasmussen et al. since one would be motivated to provide shared packet data channels optimized for packet data (lines 48-49, Col. 3 from Billstrom).

As per claim 26:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 19. Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose the remaining limitation of the claim. However, Billstrom discloses the "Apparatuses and Mobile stations for providing packet data communication in digital TDMA Cellular Systems" invention, which teaches a method of

negotiating a cipher mode during a handover process (Col 8 lines 46 to Col 9 line 20, and Col 9 lines 20 to 67).

Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art at the time of invention to incorporate Billstrom with ciphering mode teaching in Sasuta et al., Talbot, and Rasmussen et al. since one would be motivated to provide shared packet data channels optimized for packet data (lines 48-49, Col. 3 from Billstrom).

As per claims 135:

Sasuta et al., Talbot, and Rasmussen et al. disclose a system according to claim 94. Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose the remaining limitation of the claim. However, Billstrom discloses wherein the mobile communication network is a GSM network" in (Col. 1, line 62 from Sasuta et al.). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art at the time of invention to incorporate Billstrom with ciphering mode teaching in Sasuta et al., Talbot, and Rasmussen et al. since one would be motivated to provide shared packet data channels optimized for packet data (lines 48-49, Col. 3 from Billstrom).

11. Claims 32-34, 67, 69, and 144-146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, and Rasmussen et al. and further view of Lewis et al, US Patent No. 6192255, hereinafter "Lewis".

As per claims 32, 67, and 144-146:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claim 19". Sasuta et al., Talbot, and Rasmussen et al. do not disclose, "the mobile station comprises a light source the method comprising indicating the ciphering mode used in communication between the mobile communication network and the mobile station to a user of the mobile station using the light source".

However, Lewis discloses "the mobile station comprises a light source and the ciphering mode used in data communication between the mobile communication network and the mobile station is indicated with the light source" and "change of ciphering mode with flashing light and/or acoustic signal" in (Col 5 lines 10-25; Col 20 lines 10-15; and Col 16 lines 40-67).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Sasuta et al., Talbot, and Rasmussen et al. with Lewis to display the information for alerting the user.

As per claims 33 and 69:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 28 and 68". Sasuta et al., Talbot, and Rasmussen et al. do not disclose, "the mobile station comprises a display unit and an acoustic signal forming element, the method comprising indicating the ciphering mode used in communication between the mobile communication network and the mobile station to a user of the mobile station using the display unit, and indicating a change in ciphering mode to a user of the mobile station using the acoustic signal forming element".

However, Lewis discloses "the mobile station comprises a display unit and an acoustic signal forming element, the ciphering mode used in data communication between the mobile communication network and the mobile station is indicated with the display unit, and a change in ciphering mode is indicated with the acoustic signal forming element" in (Col 10 lines 53-67, Col 20 lines 10-15, and Col 16 lines 40-67).

Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate Sasuta et al., Talbot, and Rasmussen et al. with Lewis to display the information for alerting the user.

As per claim 34:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 32". Sasuta et al., Talbot, and Rasmussen et al. do not disclose, "comprising indicating a change in ciphering mode is indicated with a flashing light".

However, Lewis discloses "a change in ciphering mode is indicated with a flashing light" in (Col 20 lines 10-15, and Col 16 lines 40-67).

Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate Sasuta et al. and Talbot with Lewis to display the information for alerting the user.

12. Claims 35 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, Rasmussen et al. and further in view of Kniffin et al, US Patent No. 6072402, hereinafter "Kniffin"

As per claims 35 and 70:

Sasuta et al., Talbot, Rasmussen et al. disclose "a method and apparatus according to claims 28 and 68 characterized in that the means for indicating a change in the cipher mode by the flashing light and vibration. Sasuta et al., Talbot, Rasmussen et al. do not

teach a change in the cipher mode causing to generate vibration caused by vibration battery.

However, Kniffin discloses "Secure Entry System with Radio Communications" invention, which including a signaling means to alert the user, such as beeping, vibrating, or displaying in (Col 7 lines 10-15, and Col 10 lines 10-20).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate alert mechanism in Kniffin with Sasuta et al., Talbot, Rasmussen et al. for sensing different event and conveniently alerting the user.

13. Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, and Rasmussen et al. and further in view of Serbetcioglu et al, US Patent No. 5719918, hereinafter "Serbetcioglu",

As per claim 45:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method according to claim 44".

Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose the remaining limitation of the claim.

However, Serbetcioglu disclose "a method according to claim 44, wherein the first type of communication is a telephone call and

said second type of data communication is a short message (SMS)" in (Serbetciouglu, Col 7 lines 10-15).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Sasuta et al., Talbot, and Rasmussen et al. with Serbetciouglu to implement two types of data ciphering communication in a wireless network for simultaneously working on different types of data.

14. Claims 37-43, 75-76, 80, 87-89, 92, 125-126 and 130, 149-151, and 154-155 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, and Rasmussen et al. and further in view of Kennedy et al, European Patent No. 0680171A2, hereinafter "Kennedy".

As per claims 37, 75, 87, 125, and 149:

Sasuta et al., Talbot, and Rasmussen et al. disclose "a method and apparatus according to claims 36, 74, 86, 124, and 148". Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose "the said cipher indication memory block makes an interrupt request responsive to a detecting that a new value has been set in the cipher mode indication data field".

However, Kennedy discloses said cipher indication memory block makes an interrupt request in response to a change in the cipher mode indication data field in (Col 4, lines 8-13).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sasuta et al., Talbot, and Rasmussen et al. to incorporate Kennedy's feature to electronically controller the mode of the communication.

As per claims 38, 41, 76, 88, 92, 126, and 150:

Sasuta et al., Talbot, Rasmussen et al., and Kennedy disclose "a method and apparatus according to claims 37, 40, 75, 87, 86, 125, and 148 wherein the user interface block detects said interrupt request and sends an inquiry about the cipher mode to the cipher indicator memory block and the cipher indicator memory block returns data on the cipher mode to the user interface block in response to said inquiry" in ((Col 4 line 5 to Col 5 line 28 from Kennedy) and (Col. 3 line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.)).

As per claims 39, 40, and 43:

Sasuta et al., Talbot, Rasmussen et al., and Kennedy disclose “a method and apparatus according to claims 36, 38, and 42, wherein the user interface block is configured to set the cipher mode indicator to a mode corresponding to the cipher information provided by the cipher mode indicator memory block (Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 38; Fig. 1 from Sasuta et al.) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

As per claims 42, 80, 130, and 154:

Sasuta et al., Talbot, and Rasmussen et al. disclose “a method and apparatus according to claims 36, 74, 124, and 148, wherein the user interface block sends cipher mode inquiry message to the cipher indicator memory block about the state of the cipher mode indication data field ((Col. 3 line 24-39; Col. 3, line 60 to Col. 4 line 17; Fig. 1 from Sasuta et al.) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.)).

Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose the remaining limitation of the claim.

However, Kennedy disclose each inquiry being separated in time from the next by a predetermined interval and the cipher indication memory block is operable to return an indication of the state of the cipher mode indication data field in response to each inquiry" in (Col 4 line 5 to Col 5 line 28 from Kennedy).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the features in Kennedy to Sasuta et al., Talbot, and Rasmussen et al. to electronically control the mode of the communication.

As per claims 89, 151, and 155:

Sasuta et al., Talbot, Rasmussen et al., and Kennedy disclose "an apparatus according to claim 88, 150 and 154 wherein the user interface block is configured to set the cipher mode indicator to a mode corresponding to the cipher information provided by the cipher mode indicator memory block (Col. 3, lines 27-39; Col. 3, line 60 to Col. 4, line 38; Fig. 1 from Sasuta et al.) and (Col. 3, lines 8-25; Col. 7, lines 7-25; and Fig. 3 from Rasmussen et al.).

15. Claims 140-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, and Rasmussen et al. in view of Raith, US Patent No. 5237612, hereinafter "Raith".

As per claims 140:

Sasuta et al., Talbot, and Rasmussen et al. disclose a mobile station according to claim 139. Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose wherein the mobile station is configured to determine the ciphering mode to be used in communication between the mobile communication network and the mobile station by performing a location update procedure. However, Raith discloses wherein the mobile station is configured to determine the ciphering mode to be used in communication between the mobile communication network and the mobile station by performing a location update procedure (Col. 2, line 67 to Col. 3, line 11; Col. 17, lines 5-34; Col. 19, lines 46-61 from Raith).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sasuta et al., Talbot, and Rasmussen et al. incorporate Raith's teaching to provide adaptable authentication of a mobile station within a radio network.

As per claims 141:

Sasuta et al., Talbot, and Rasmussen et al. disclose a mobile station according to claim 136. Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose wherein the mobile station is configured to determine a ciphering mode to be used in communication between the mobile communication network and the mobile station during a communication handover procedure that occurs when the mobile station moves between a first part of the mobile communication network and a second part of the mobile communication network.

However, Raith discloses wherein the mobile station is configured to determine a ciphering mode to be used in communication between the mobile communication network and the mobile station during a communication handover procedure that occurs when the mobile station moves between a first part of the mobile communication network and a second part of the mobile communication network (Col. 2, line 67 to Col. 3, line11; Col. 17, lines 5-34; Col. 19, line 46 to Col. 20, line 14 from Raith).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sasuta et al., Talbot, and Rasmussen et al. incorporate Raith's teaching

to provide adaptable authentication of a mobile station within a radio network.

16. Claim 147 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot, and Rasmussen et al. in view of Fujiwara et al., US Patent No. 5266947, hereinafter "Fujiwara".

As per claims 147:

Sasuta et al., Talbot, and Rasmussen et al. disclose a mobile station according to claim 142, wherein the mobile station is configured to indicate a change in ciphering mode. Sasuta et al., Talbot, and Rasmussen et al. do not expressly disclose causing vibration battery to vibrate is used to indicate mode change.

However, Fujiwara discloses that the event occurs (i.e., changing mode of operation) can be associated with vibration (Col. 3, lines 7-23 from Fujiwara).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sasuta et al., Talbot, and Rasmussen et al. to incorporate Fujiwara's teaching to provide notification to a mobile station when certain event occurs.

Note: Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

17. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

- a. Mauger et al. (U.S. Patent 5,260,987) disclose a base station controller (BSC) personal communications network (PCN), which

can for example be based on GSM, has associated with it a local PSTN network and is such that local calls between mobile subscribers and the local PSTN network can be made without involving a remote mobile-services switching centers (MSC), thereby permitting a cheap local call tariff to be employed whilst preserving the interfaces e.g. the GSM Abis and A interfaces. The BSC is intelligent and includes a BSC function, a local MSC function and a location register which slaves mobile subscriber location information from the MSC location registers.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw, whose telephone number is (571) 272-8593. The examiner can normally be reached on Monday-Friday from 9:30 AM - 6:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on 571-272-7884.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Art Unit: 2439

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Nov. 20, 2009

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439